Choice of measurement basis as signal

A. Kalev
Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, 117543, Singapore

A. Mann and M. Revzen
Department of Physics, Technion - Israel Institute of Technology, Haifa 32000, Israel
(Dated: December 3, 2012)

In classical mechanics, performing a measurement without reading the measurement outcome is equivalent to not exploiting the measurement at all. A non-selective measurement in the classical realm carries no information. Here we show that the situation is remarkably different when quantum mechanical systems are concerned. A non-selective measurement on one part of a maximally entangled pair can allow communication between two parties. In the proposed protocol, the signal is encoded in the *choice* of the measurement basis of one of the communicating parties, while the outcomes of the measurement are irrelevant for the communication and therefore may be discarded. Different choices for the (non-selective) measurement basis correspond to different signals. The scheme is studied in a Hilbert space of odd prime dimension.

PACS numbers: 03.65.Ta;03.67.Hk

I. INTRODUCTION

One of the aims of quantum information theory is to harness features of quantum systems for implementing tasks which otherwise would not be possible to implement. In this contribution we utilize a feature that to the best of our knowledge was not utilized before for quantum information tasks, in particular for encoding and transmitting information. This feature is non-selective measurements on quantum systems. In such measurements the outcomes are not recorded, and therefore it is surprising that one would be able to use this kind of measurements for communication tasks. Indeed non-selective measurements on classical systems do not carry information, nor can be used for communication [1, 2]. Here we show how non-selective measurements on one quantum system of a maximally entangled pair, can used to encode and eventually communicate information. In the proposed protocol the *basis, i.e. the choice*, of the (non-selective) measurement is the signal. The outcomes of the measurement are totally irrelevant and may be discarded.

Confining our study to a Hilbert space of dimension d=prime $\neq 2$, we consider as alternative choices for measurements the alternative mutual unbiased bases (MUB). For prime dimension there are $d+1$ MUB [3–8]. A possible set of d+1 MUB can be defined as follows. The first basis is the computational basis $\{|n\rangle\}_{n=0}^{d-1}$, composed of the d orthonormal eigenstates of the generalized Pauli operator $\hat{Z}$, $\hat{Z}|n\rangle = \omega^n|n\rangle, |n+d\rangle = |n\rangle, \omega = e^{i\frac{2\pi}{d}}$. The other d orthonormal bases are parametrized by b=0, 1, . . . , d−1. The kets that compose the d remaining bases are given in terms of the computational basis by [6],

$$|m;b\rangle = \frac{1}{\sqrt{d}}\sum_{n=0}^{d-1}|n\rangle\omega^{\frac{b}{2}n(n-1)-nm},\ b,m=0,1,\ldots,d-1. \tag{1}$$

We shall designate the computational basis by $b = \ddot{0}$, and depending on the context we may also denote the kets of the computational basis $|m\rangle$ by $|m;\ddot{0}\rangle$. Thus, the d+1 bases are labelled by $b = \ddot{0}, 0, 1, \ldots, d-1$.

The proposed communication protocol is described in detail in Sec. II. We assume that the two communicating parties, Alice and Bob, agree beforehand upon a code, associating messages with the parameters, b, specifying the MUB. There is no classical communication between Alice and Bob beyond this point. The protocol involves a two d-level system (qudit) entangled state prepared by Alice with one qudit availed to Bob who wishes to communicate a message, $b = \ddot{0}, 0, 1, \ldots, d-1$, to Alice. To this end Bob measures the part of the system availed to him in the basis parametrized with the b of his message. He must complete his measurement yet may ignore its outcome(!) and then return the qudit to Alice. Now Alice measures the two-qudit resultant state and deduces, almost always, the basis b used by Bob, hence decodes the message. The procedure is quantal in that the signal corresponds to the *basis* of Bob's measurement, that is to the "alignment" of his instrument, and in that the measurement outcomes are irrelevant and may be unrecorded. The last section, Sec. III, contains some concluding remarks.

II. CHOICE OF MEASUREMENT BASIS AS SIGNAL

To establish a communication channel, let Alice prepare one of the following d^3 two-qudit maximally entangled states [9, 10],

$$|c, r; s\rangle_{1,2} = \frac{1}{\sqrt{d}} \sum_{n=0}^{d-1} |c+n\rangle_1 |c-n\rangle_2 \, \omega^{sn^2-2rn}, \tag{2}$$

with $c, r, s = 0, 1, \ldots, d-1$, and send one of the qudit, say, the one labelled by 1, to Bob. We note that, for a given s value, these states form an orthonormal, maximally entangled, basis for the Hilbert space of the two qudits. Thus, s labels the basis and c and r label the d^2 orthonormal states within a basis.

The reduced state for Bob's qudit is the completely mixed state. To communicate a message to Alice, Bob measures his qudit in one of the MUB labeled by $b = \ddot{0}, 0, 1, \ldots, d-1$. The message is his choice of the basis used for the measurement. Bob may or may not record the measurement outcome. This is of no relevance to the protocol. After completing his non-selective measurement, Bob sends the qubit back to Alice. The two-qudit state is described now by

$$\rho_{1,2} = \frac{1}{d} \sum_{m=0}^{d-1} |m; b\rangle_1 \langle m; b| c, r; s\rangle_{1,2} \langle c, r; s| m; b\rangle_1 \langle m; b| \tag{3}$$

To retrieve the message, Alice now measures the two qudits in the basis of preparation, $\{|c', r'; s\rangle_{1,2}\}_{c',r'=0}^{d-1}$ of Eq. (2). The probability to obtain an outcome which corresponds to the basis state $|c', r'; s\rangle_{1,2}$ is

$$\langle c', r'; s|\rho_{1,2}|c', r'; s\rangle_{1,2} = \frac{1}{d^2} \begin{cases} \delta_{c,c'} & \text{for } b = \ddot{0} \\ \delta_{(b-s)c+r,(b-s)c'+r'} & \text{for } b = 0, 1, 2, \ldots, d-1. \end{cases} \tag{4}$$

The arithmetics is modulo d. According to the above equation, based on the outcome of her measurement, Alice can decode the message sent from Bob, that is, the basis of his measurement. If the outcome corresponds to a state $|c', r'; s\rangle_{1,2}$ with $c \neq c'$, Alice infers that $b = s + \frac{r'-r}{c-c'}$. Since she knows the values of c, r, c', r' and s, she can calculate the message b. If, on the other hand, $c = c'$ and $r \neq r'$ Alice infers that $b = \ddot{0}$. The case of $c = c'$ and $r = r'$ is inconclusive for Alice. The inconclusive outcome occurs with probability $1/d^2$. In that case the preparation state and the detection state of the two qudits is the same and she does not gain any information about Bob's message. Hence the decoding table is,

$$\begin{aligned} c \neq c' &\;\rightarrow\; b = s + \tfrac{r-r'}{c'-c} \\ r \neq r',\ c = c' &\;\rightarrow\; b = \ddot{0} \\ r = r',\ c = c' &\;\rightarrow\; \text{inconclusive.} \end{aligned} \tag{5}$$

III. CONCLUDING REMARKS

To conclude, we showed how non-selective measurements in MUB on one part of an entangled pair could be used to encode information. The scheme uniquely utilizes quantum features of the system, since performing non-selective measurements on classical systems (no matter how correlated they are) cannot carry or manipulate information [1, 2]. In this protocol, by sending a qudit, Bob is able to transfer, on average, more than $\log_2 d$ bits of information to Alice. This is, in some respect, a form of dense coding. We note for comparison that super-dense coding achieves $2 \log_2 d$ bits per qudit sent from Bob to Alice [11]. However, in the super-dense coding scheme [11] unitary transformations are used for the encoding, while here non-selective measurements are utilized. This protocol exemplifies how tasks which seem impossible by classical reasoning are realized in quantum systems.

Acknowledgments

The Centre for Quantum Technologies is a Research Centre of Excellence funded by the Ministry of Education and by the National Research Foundation of Singapore.

[1] J. Schwinger, Quantum mechanics: symbolism of atomic measurements, B.-G. Englert (Ed.), (Springer, Berlin Heidelberg 2001)
[2] L. Diósi, A Short Course in Quantum Information Theory, Lect. Notes Phys. 827, 2nd edition (Springer, Berlin Heidelberg 2011).
[3] I. D. Ivanovic, J. Phys. A, **14**, 3241 (1981).
[4] A. Vourdas, Rep. Math. Phys. **40**, 367 (1997).
[5] W. K. Wootters and B. D. Fields, Ann. Phys. (N.Y.) **191**, 363 (1989).
[6] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury and F. Vatan, Algorithmica **34**, 512 (2002).
[7] K. S. Gibbons, M. J. Hoffman and W. K. Wootters, Phys. Rev. A **70**, 062101 (2004).
[8] A. Vourdas, Rep. Prog. Phys. **67**, 267 (2004).
[9] M. Revzen, Phys. Rev. A **81**, 012113 (2010).
[10] M. Revzen, arXiv:1111.6446 (2011).
[11] C. H. Bennett and S. J. Wiesner. Phys. Rev. Lett., **69** 2881 (1992).